

ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)
)

Policies and Rules Concerning)
Toll Fraud)
_____)

CC Docket No. 93-292

RECEIVED

FEB 10 1994

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

REPLY COMMENTS
OF
SPRINT CORPORATION

Jay C. Keithley
Norina T. Moy
1850 M St., N.W., Suite 1110
Washington, D.C. 20036
(202) 857-1030

Craig T. Smith
P.O. Box 11315
Kansas City, MO. 64112
(913) 624-3065

February 10, 1994

No. of Copies rec'd
List ABCDE

026

TABLE OF CONTENTS

Summary	ii
I. INTRODUCTION	1
II. TOLL FRAUD LIABILITY SHOULD BE ASSIGNED ON THE BASIS OF EACH PARTY'S ABILITY TO CONTROL SUCH FRAUD OR ITS FAILURE TO UNDERTAKE REASONABLE FRAUD CONTROL EFFORTS	2
1. PBX Fraud	3
2. Payphone Fraud	8
3. Alternative Billing Service/LIDB Fraud	12
4. Cellular Fraud	16
III. CONCLUSION	17

Summary

The controversy in the instant proceeding centers on how, or whether, to assign liability for toll fraud among different parties. The most the Commission should do in this regard is to adopt the broad principle that liability should be borne by the party at fault or by the party in the best position to prevent and detect such fraud.

In general, application of this principle would assign liability as follows:

- PBX owners would be liable for fraud committed through their equipment;
- private payphone providers would be liable for fraud committed over their payphones, provided that blocking and screening services provided by the LEC work as intended and provided that the IXC seeks (e.g., through a LIDB query), accepts, and properly uses the blocking and screening information;
- LIDB providers accept liability for fraud resulting from failure to meet agreed-upon operational standards, provided that another party is not at fault for failing to exercise reasonable fraud control mechanisms of its own;
- IXCs accept liability for fraud resulting from their failure to perform a LIDB query and for fraud committed using their proprietary calling card;
- cellular carriers accept liability for all airtime charges associated with a fraudulent cellular call, for any toll charges for cellular calls which only the cellular carrier can validate, and for fraud which results from cloned ESNs.

This principle is reasonable, equitable, and more readily implemented than other rules suggested by commenting parties, and thus should be adopted by the Commission.

FEB 10 1994

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of

Policies and Rules Concerning
Toll Fraud

CC Docket No. 93-292

REPLY COMMENTS

Sprint Corporation ("Sprint"), on behalf of Sprint Communications Company LP ("Sprint Long Distance"), the United and Central Telephone Companies ("United Telephone"), and Sprint Cellular, hereby respectfully submits its reply to comments filed in the above-captioned notice of proposed rulemaking ("NPRM").

I. INTRODUCTION.

There is widespread agreement among parties filing comments in this proceeding on the following points:

- that the problem of telecommunication toll fraud is a serious one, and that toll fraud may be minimized, but will never be completely eliminated or avoided, no matter how comprehensive carriers' and customers' toll fraud detection and prevention systems are;
- that specific federal legislation needs to be enacted to make all telecommunications fraud a crime, and that more resources need to be devoted to law enforcement efforts;
- that the Commission should become more actively involved in industry efforts to prevent and minimize toll fraud, either through existing industry organizations such as the Toll Fraud Prevention Committee and the Communications Fraud Control Association, or through a new Federal Advisory Committee;
- that customer education about the risks of toll fraud and how to prevent it is vital, and that IXCs,

LECs, equipment manufacturers and vendors, etc., should continue and further enhance their anti-fraud efforts.¹

In contrast, the issue of how (or whether) to assign liability for toll fraud among different parties is more contentious. As discussed below, the most the Commission should do in this regard is to adopt the general principle that liability for toll fraud should be borne by the party at fault or by the parties in the best position to control such fraud.

II. TOLL FRAUD LIABILITY SHOULD BE ASSIGNED ON THE BASIS OF EACH PARTY'S ABILITY TO CONTROL SUCH FRAUD OR ITS FAILURE TO UNDERTAKE REASONABLE FRAUD CONTROL EFFORTS.

Most commentators seem to agree that toll fraud liability should be assigned based on the ability of each party (customer, carrier, vendor, etc.) to control such fraud. However, parties disagree as to their own relative ability to control fraud, and many parties espouse the liability apportionment principle only insofar as it will shift their own burden to

¹AT&T suggests (p. 4) that the Commission require all carriers collectively to distribute an annual notice to all customers and to new subscribers regarding toll fraud. While Sprint has no objection if AT&T wishes to do a billing insert, the Commission should not require all carriers to do so. Many customers tend to ignore extra inserts in their bills, and it is unclear what the cost of doing this kind of mass mailing would be. Sprint believes that its current customer education efforts (including written and oral presentations to customers, brochures and notices issued on its own and in conjunction with organizations such as the National Association of Consumer Agency Administrators, industry fora participation, etc.) are more effective than a mass-mailed billing insert. Sprint further believes that carriers should retain the flexibility to implement whatever customer education efforts they consider best.

another entity, or at least not increase their existing liability. For example, CPE owners and private payphone providers feel that LECs and IXCs should accept some (even most) of the toll fraud losses; some equipment vendors believe that they should never be held liable for fraud committed using CPE which they manufactured or sold; some LIDB providers feel that they should be liable only when they are grossly negligent or engage in willful misconduct; and some IXCs in turn believe that they should be fully indemnified by LIDB providers for their (IXCs') tariffed charges if they provide the LIDB provider with called/calling number information. As discussed below, the general guideline for apportioning liability noted above--that liability should reflect fault and ability to control fraud--can be reasonably applied in most situations involving toll fraud. Any attempt to adopt specific rules to govern liability in specific situations inevitably will be incomplete, subject to fierce disputes, and, eventually, out-of-date, and should therefore be avoided.

1. PBX Fraud

PBX owners and users groups are virtually unanimous in urging that LECs and IXCs share liability for CPE fraud.² They argue that carriers are better able to monitor unusual

²See, e.g., Ad Hoc; Arinc; API; Communications Managers Association, New York Clearing House Association, and the Securities Industry Association ("CMA"); FMC; Tele-Communications Association; Utilities Telecommunications Council ("UTC"); International SL-1 Users Association; and form letters submitted by various parties.

traffic patterns from CPE systems, and that carriers should offer various fraud prevention services as part of basic service (i.e., at no additional charge), or at most at "cost-based" rates. Various of these parties also assert that current policy, which assigns liability for CPE fraud to the CPE owner, gives IXCs and LECs little incentive to "assist customers in combatting CPE-based fraud, or even to alert them to vulnerabilities in the use of CPE or services."³

Sprint sympathizes with the concerns of PBX owners and business customers. However, as many other parties point out,⁴ it is the PBX owner who controls access to and use of the CPE; who decides whether to use various PBX features which are susceptible to fraud (such as the remote access feature)⁵;

³CMA, p. 4; see also, API, p. 6; UTC, p. 2.

⁴See, e.g., AT&T, p. 11; Comptel, p. 2; IXC Toll Fraud Subcommittee ("IXC TFS"), p. 3; MCI, p. 5; Nynex, p. 17; Rochester, p. 2; SWB, p. 3; Telecommunications Resellers Association, p. 5; Teleport, p. 5; USTA, p. 3; Wiltel, p. 2.

⁵Ad Hoc also discusses another type of remote access fraud--"network-based" fraud in which a user dials an 800 number, enters an access code, and then makes an outgoing call. Ad Hoc states that IXCs, not customers, have the "ultimate power to...detect and thwart fraud using network-based remote access services" (p. 3) and thus should be liable for such fraud. Although Ad Hoc would have IXCs accept responsibility for this type of fraud, it would not allow the carrier to "unilaterally shut down numbers upon even the slightest suspicion that something is amiss" (p. 3, n. 2). Ad Hoc cannot have it both ways. If it believes that IXCs can control the fraud and should accept liability, it must also grant them the latitude to take the steps necessary to control such fraud. In cases where Sprint Long Distance can detect fraud and accepts liability (e.g., for its calling cards), it reserves the right to disable--on its own authority--any code which it suspects is being abused. Although Sprint Long

(Footnote Continued)

who chooses what PBX and adjunct equipment and software to use;⁶ and who is the only one actually able to identify whether traffic from his PBX is legitimate or fraudulent (carriers can only identify abnormal traffic patterns). Customers can and should also perform routine audits and system monitoring, using, for example, the station message detail reporting capability which is standard in most PBX equipment. In general, CPE owners should accept responsibility for the fraud that results from their failure to exercise such control.⁷

Contrary to the recommendations of users, IXC's and LEC's should not be required to offer fraud monitoring and detection services as part of basic service. Carriers--especially interexchange carriers--are subject to market pressures to provide these services, and in fact a number of fraud monitoring and protection services (such as SprintGUARD (TM) and SprintGUARD Plus (TM),⁸ AT&T NetProtect (TM), MCI Detect (TM))

(Footnote Continued)

Distance makes every effort to contact its customers where feasible before disabling a code, it is sometimes not possible to reach the customer in a timely fashion.

⁶Manufacturers offer a range of different security features with their equipment. See, e.g., Ericsson, p. 3; Northern Telecom, p. 2; TeleDesign, p. 1; Xiox, p. 3.

⁷Of course, the financial liability of customers who subscribe to services such as SprintGUARD Plus (TM) is limited.

⁸SprintGUARD (TM) service (which includes technical assistance, traffic monitoring and analysis, training courses and on-going security support) is available at no extra charge, and SprintGUARD Plus (TM) (which limits the customer's financial exposure) is available for a reasonable fee.

are already available. Customers who are risk-averse, or believe that they are vulnerable to CPE fraud, are easily able to obtain additional fraud protection from a carrier which offers such services. If its existing carrier does not offer the desired services, a customer may choose to move its account to another carrier which does offer them.

Moreover, universal monitoring services such as those which users groups are apparently requesting are resource-intensive. Establishing customer-specific fraud thresholds is even more difficult to implement. While Sprint Long Distance is able to offer SprintGUARD to all Sprint Long Distance business customers as a means of distinguishing its service in the competitive market, other carriers may lack the financial or other resources, or the market differentiation plans, to develop and implement similar services.⁹ Moreover, parties urging that monitoring and other fraud prevention services be considered part of basic service should be aware that carriers likely will spread the costs of providing such services across the rates charged to all of their customers, including those who have little need or desire for them. It is far more efficient and fair to allow customers who do need or want additional or specialized toll fraud protection to choose optional protective services (based upon their relative costs and benefits), than to force all customers (including those

⁹ See, e.g., Teleport, pp. 4-6.

who do not need or want additional fraud protection) to bear some portion of the cost of such services.

Finally, it is simply not the case that carriers have no incentive to provide CPE (or any other type of service or equipment) fraud prevention services. Many IXCs and LECs detailed their extensive efforts to combat CPE fraud.¹⁰ They invest in these costly efforts to promote customer goodwill, to respond to marketplace demands, and to avoid or minimize the financial burden of toll fraud.¹¹ These factors provide strong incentives for carriers to take steps to prevent CPE fraud.¹² While some commenting parties may feel that IXCs are

¹⁰See, e.g., Sprint, pp. 3-5 and Attachments A and B; AT&T, pp. 3, 9-10 and Appendix A; BellSouth, pp. 3-4; GTE, Attachment A; MCI, pp. 3, 9 and Attachment A; Nynex, pp. 3-8; Pacific, pp. 5-7 and Exhibit B; US West, pp. 10-29.

¹¹There are many financial costs associated with fraudulent calls. First, even though current policy usually holds the CPE owner liable, if the carrier is unable to collect its bill, its uncollectible expense will increase. Second, carriers incur various costs (including access, billing and collection, and network expenses) to carry the fraudulent calls irrespective of whether payment is made by the customer whose account has been compromised or by a perpetrator who has established an account for the purpose of committing fraud. Third, personnel costs alone can be quite expensive: customer service, fraud prevention operations, corporate security, account team, and sometimes regulatory personnel all may become involved in a toll fraud investigation or complaint.

¹²If, contrary to Sprint's recommendations, the Commission decides to require IXCs to provide certain anti-fraud services (mandatory monitoring, prescribed customer education programs, etc.), such requirement should apply to all IXCs, both facilities-based and resellers. If the Commission believes that such services are necessary to protect customers, then customers of all IXCs and resellers should be afforded the same protection.

not doing "enough" to prevent fraud, it is important to realize that it is impossible to completely eradicate CPE or any other kind of fraud. Even the most sophisticated monitoring system will detect abnormal activity only after a threshold has been reached, and fraud perpetrators constantly find new ways to evade existing fraud detection systems and to trick (e.g., by posing as an FBI agent or employee of "the telephone company" investigating fraud) the end user into revealing proprietary account information (a practice known as "social engineering" with the end user).

2. Payphone Fraud

Like CPE owners, numerous private payphone owners assert that LECs and IXC's should be required to accept a greater (even the greatest) degree of liability for fraud.¹³ They urge federal adoption of the Florida rule, under which payphone owners are absolved of liability for payphone fraud so long as they subscribe to LEC-provided OLS (originating line screening) and BNS (billed number screening) services. Indeed, at least two parties would go even further. APCC states (p. 23) that a carrier which "fails to provide adequate fraud monitoring should not be able to hold a payphone owner liable, even if the payphone owner does not subscribe to blocking and screening

¹³See, e.g., American Public Communications Council ("APCC"); the Florida Pay Telephone Association; Independent Payphone Association of New York ("IPANY"); Massachusetts Payphone Association; New Jersey Payphone Association ("NJPA"); South Carolina Office of Information Resources, p. 5.

services," and the NJPA (p. 4) would require payphone owners to subscribe to OLS/BNS only where the rate is "reasonable." Payphone owners argue that having taken "reasonable" steps to prevent fraud, they should then be absolved of any further responsibility.

As US West points out (p. 43), payphones are a type of CPE. Payphone owners, like other CPE owners, are in the best position to prevent fraud: they decide what equipment to install, what services (e.g., blocking and screening) to use, and what physical security measures to take. Moreover, payphone owners know, or should know, that fraud is one of the risks of their business. It makes no sense for payphone owners to expect to reap the rewards of offering service without accepting the attendant risks as well, and it is unreasonable for payphone owners to expect LECs and IXC's to completely protect the payphone owner against such risks. A rule such as Florida's allocates liability arbitrarily, and ignores the many other steps which payphone providers can take to prevent fraud. Therefore, it should not be adopted on a national level.

This is not to say that LECs and IXC's should never be liable for payphone fraud. Sprint believes that where the blocking and screening services do not reasonably perform as intended, or where the blocking and screening information (including ANI II digits and payphone "cuckoo" tones) is negligently ignored or misused, the LEC or IXC (as appropriate) should be responsible for any resulting fraud. However, based upon the payphone provider's own ability to detect and control

fraud, it is unreasonable for payphone owners to rely solely upon carrier-provided blocking and screening services to prevent fraud.

Despite the assertions of some payphone owners, subscription to OLS and BNS is not the only fraud prevention measure which payphone owners can take. They can also:

- use the "no PIC" option, where available;
- block 10XXX 1+ calls, at either the CPE (using "smart" payphones) or LEC central office;
- install payphones which generate a special "cuckoo" tone or announcement identifying the line as a payphone;
- block international calling from their phones;
- subscribe to available LEC blocking and screening services (besides OLS and BNS, LECs offer international direct dial blocking (IDDB) service, and at least one LEC, BellSouth, offers "high toll indicator service," under which the LEC notifies the payphone owner if toll usage exceeds a specified dollar amount). At least some payphone owners currently do not subscribe to the LECs' OLS and BNS services even when they are available free of charge; subscription rates to IDDB services are believed to be even lower;¹⁴
- place their payphones in physically secure spots to help minimize "clip on" fraud and "shoulder surfing" and to allow the payphone owner to monitor use of the payphone;
- block incoming calls, at least to public (although perhaps not semi-public) payphones;
- refrain from storing PIN numbers for calling cards in billing records that are often contained in the remote access CPE.

¹⁴See, e.g., Sprint, p. 11; APCC, p. 18; Bell Atlantic, p. 4; GTE, p. 9; Nynex, p. 21.

Other parties also can take steps to help reduce payphone fraud. For example:

- where possible, LECs should assign, and payphone owners should accept, payphone numbers in the 8000 or 9000 series. This would enable international operators to identify a terminating number as a payphone, and, where the caller has requested collect or third party billing to such a number, the operator can request that the caller select an alternative billing mechanism;¹⁵
- where the capability exists, the originating LEC should send, and the IXC should accept, the standard ANI II digits which identify the line as a payphone;
- IXCs and OSPs should do a LIDB query on each alternatively billed call to prevent collect calls to a payphone and use of payphone lines as the billed third party;
- LECs should continue to work on mechanisms to prevent dial tone reorigination;
- LECs should endeavor to place payphone network interfaces in physically secure spots to minimize unauthorized access and "clip-on" fraud.¹⁶

Sprint reiterates that even if all of the measures listed above are taken, if all of the fraud protection services work as intended, and if all parties do what they are supposed to

¹⁵ See, e.g., Sprint, p. 12; APCC, p. 22; AT&T, p. 26; BellSouth, p. 9; MCI, p. 10.

Sprint would caution that use of 8000-9000 numbers is only a stop-gap measure, and will not prevent fraud in currently subscribed payphones unless such payphones are reassigned to the 8000-9000 series. Moreover, some non-payphone customers have already been assigned 8000-9000 numbers, and any reassignment (to the extent practical) must occur over time.

¹⁶ LECs cannot guarantee the physical security of payphone network interface locations because such interfaces and phones are on customer premises and the customer often dictates placement of the interface and may control access to the area where the interface is installed.

do, some payphone fraud will still occur. While unfortunate, this type of fraud is simply a fact, and a cost, of offering payphone service. Payphone providers should therefore be liable for such fraud. While it may indeed be the case that potential fraud losses are "a serious threat to every IPP [independent public payphone] provider's ability to continue doing business" (APCC, p. 2), this threat is simply a factor which every payphone owner must consider in deciding whether and where to offer service.

3. Alternative Billing Service/LIDB Fraud

As Sprint discussed in its comments (pp. 14-23), it is critical that LIDB providers (both LECs and non-LECs) commit to and be held accountable for compliance with specific operational service standards developed jointly with their LIDB customers. These standards should cover items such as establishment and use of trigger thresholds, procedures for handling fraud referrals, maintenance of the database under normal and emergency conditions, and sharing of customer information needed to prevent or investigate fraud.

The discussion over LIDB-related fraud centered around the assignment of liability for fraud and the provision by IXCs of calling and called numbers with each LIDB query. While there was general agreement on various points such as the importance of calling and called number as a fraud prevention tool and the need to perform a LIDB query on every alternatively billed call, there was substantial disagreement over the appropriate standard for LIDB provider liability.

In their comments, the three largest IXCs expressed some willingness to provide the calling and called numbers with each LIDB query.¹⁷ There seems to be little dispute that when LIDBs are consistently queried, this information would enhance LIDB's fraud deterrence capabilities because LIDB providers would be able to more thoroughly analyze usage spikes when thresholds are exceeded on individual calling cards and in different originating and terminating locations, as well as unusual usage patterns such as multiple origination points. Calling and called number information could also be used for future anti-fraud capabilities such as domestic-only LEC calling cards and call screening based on originating and/or terminating numbers.¹⁸

AT&T (p. 34) and MCI (p. 14) argue that IXCs which launch a LIDB query containing calling and called number information should be indemnified by the LIDB provider against loss of their tariffed charges for any fraudulent call authorized by the LIDB. Sprint agrees that LIDB providers which receive calling and called number information are capable of a higher standard of fraud prevention and protection than is currently the case, and that LIDB providers should accordingly commit to

¹⁷ See Sprint, pp. 18-19; AT&T, pp. 32-34; MCI, p. 14; IXC TFS, p. 15 (willing to provide originating and terminating NPA-NXX). LECs and LIDB providers all state that they want and need this information (see, e.g., Bell Atlantic, p. 8; BellSouth, p. 12; GTE, pp. 19-21; Nynex, p. 25; Pacific, p. 17; SNET, p. 7; SWB, p. 11; US Intelco, p. 2; US West, p. 25).

¹⁸ "Domestic-only" cards are feasible only if all querying companies provide originating and terminating information.

whatever operational standards are developed by the industry. LIDB providers should be responsible for fraud when established trigger thresholds have been exceeded and another party is not at fault by failing to exercise reasonable fraud control mechanisms of its own. Under these conditions, LIDB providers should repay the LIDB customer for the customer's out-of-pocket costs (LIDB query and other access charges, billing and collection fees, international settlement payments, network costs, etc.) rather than for its full tariffed rate.

Despite the reasonableness of this compromise position, most LIDB providers continue to insist on a lesser standard of liability. At the farthest extreme, US Intelco insists (p. 3) that "there is no basis for assigning liability to the LIDB provider, in the absence of willful misconduct or gross negligence." USTA (p. 5) and SWB (p. 11) assert that LIDB was not designed to and cannot prevent fraud, and that LIDB providers should therefore not be assigned liability, at least for unauthorized card use. Other LECs state that, except in cases of gross negligence or willful misconduct, their liability should be limited to a refund of the charge for the service which did not work.¹⁹ BellSouth (p. 13) goes slightly farther, stating that it will not assess any access or billing

¹⁹ See, e.g., Puerto Rico Telephone Company, p. 2; Rochester, p. 9; US West, pp. 31-36.

and collection charges when it is at fault, but that it will not reimburse the IXC for any of its other costs.²⁰

Sprint agrees with LECs which assert that they should not be required to share in the liability for fraud which occurs because of some omission on the part of the IXC (e.g., if the IXC fails to perform a LIDB query for every alternatively billed call, or if it ignores the screening information which it does receive²¹), or when the LEC is otherwise not at fault. Assigning liability to the LIDB provider in those situations is arbitrary and contrary to the general principle that liability should be based on each party's ability to control the fraud. However, what is at issue here are situations in which the fraud occurs because of a negligent error or omission on the LIDB provider's part.²² LIDB providers which do not satisfy agreed-upon operational standards are liable for at least some (depending upon whether other parties are also at fault) of any resulting fraud.

²⁰Nynex states (p. 21) that it would reimburse IXCs for access charges paid on fraudulent toll calls caused by the failure of Nynex's OLS and BNS services. It does not specify whether it would apply this same principle to other failures in LIDB service.

²¹Sprint would emphasize that the IXC needs to know in detail the exact conditions under which a specific LIDB response will be generated.

²²Current United LIDB rates do not reflect the cost of fraud losses assigned to it.

4. Cellular Fraud

There was general agreement among parties who addressed the cellular fraud issue that steps can be taken which would reduce the incidence of cellular fraud. First, virtually all parties agreed that the Commission should adopt new Part 22 rules which prohibit the manufacture or alteration of cellular phones in a way which facilitates tumbling and cloning fraud (e.g., by allowing the phone's unique electronic serial number (ESN) to be altered or removed), and that the Commission should contribute to efforts to enact legislation making cellular (as well as all other types of telecommunications) fraud a federal crime.²³ Second, cellular carriers should perform pre-call validation on every cellular call.²⁴ Third, cellular carriers should transmit to the IXC the ANI information digits which identify the call as originating from a cellular phone to facilitate IXC monitoring of cellular traffic.²⁵

In situations in which the cellular carrier is the only entity able to validate the call, the cellular carrier should accept full liability for any cellular fraud. If the IXC to which the cellular carrier passes a toll call cannot validate the ANI of the phone from which the call was made, it cannot

²³See, e.g., Sprint, pp. 12-13; AT&T, p. 30; Bell Atlantic, p. 11; CTIA, pp. 6-7; McCaw, pp. 9, 14-17; Nynex, p. 23; SWB, p. 9; Vanguard Cellular, p. 8.

²⁴See, e.g., Sprint, p. 13; McCaw, p. 6; SWB, p. 9.

²⁵See, e.g., Sprint, p. 13; MCI, p. 13.

determine whether a cellular call is legitimate or fraudulent, and thus no liability should accrue to the IXC. However, if the IXC is able to validate the call, it should accept liability for its toll charges (but not the cellular carrier's airtime charges) for fraudulent calls which result from a failure to validate.

AT&T (p. 31) and MCI (p. 13) state that fraud which results from cloned ESNs should be borne by the cellular carrier. Sprint agrees. This type of fraud is the result of cellular technology, is one of the risks of being in the cellular business, and is outside the control of the IXC. Because the cellular carrier is in the best position to control cloning, it should accept liability for this type of fraudulent traffic. Of course, if the cellular carrier is to be responsible for cloning fraud, it should also have the latitude to deactivate, on its own authority, a compromised ESN, without being held liable for wrongful termination of service.

III. CONCLUSION.

The Commission should adopt the broad principle that toll fraud liability should be borne by the party at fault or the parties in the best position to prevent and detect such fraud. In general, application of this principle would assign liability as follows:

- PBX owners would be liable for fraud committed through their equipment;
- private payphone providers would be liable for fraud committed over their payphones, provided that blocking and screening services provided by the LEC


work as intended and provided that the IXC seeks (e.g., through a LIDB query), accepts, and properly uses the blocking and screening information;

- LIDB providers accept liability for failure to meet agreed-upon operational standards, provided that another party is not at fault by failing to exercise reasonable fraud control mechanisms of its own;
- IXCs accept liability for fraud resulting from their failure to perform a LIDB query and for fraud committed using their proprietary calling card;
- cellular carriers accept liability for all airtime charges associated with a fraudulent cellular call, for any toll charges for cellular calls which only the cellular carrier can validate, and for fraud which results from cloned ESNs.

This principle is reasonable, equitable, and more readily implemented than other rules suggested by commenting parties, and thus should be adopted by the Commission.

Respectfully submitted,

SPRINT CORPORATION


Jay C. Keithley
Norina T. Moy
1850 M St., N.W., Suite 1110
Washington, D.C. 20036
(202) 857-1030

Craig T. Smith
P.O. Box 11315
Kansas City, MO. 64112
(913) 624-3065

February 10, 1994

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing **REPLY COMMENTS OF SPRINT CORPORATION** was sent by United States first-class mail, postage prepaid, on this the 10th day of February, 1994, to the below-listed parties.

Kathleen B. Levitz
Acting Chief
Common Carrier Bureau
Federal Communications Comm.
1919 M Street, N.W.
Room 500
Washington, D.C. 20554

Linda Dubroff
Common Carrier Bureau
Federal Communications Comm.
2025 M Street, N.W., Room 6008
Washington, D.C. 20554

International Transcription
Service
1919 M Street, N.W., Room 246
Washington, D.C. 20554

Albert Kramer
Robert Aldrich
Dana Lesemann
Keck, Mahin & Cate
1201 New York Avenue
Penthouse Suite
Washington, D.C. 20005
Counsel for APCC

Randall Collett
Assn. of College and Universities
Telecommunications Administrator
250 Main Street
Suite 2420
Lexington Financial Center
Lexington, KY 40507

Mark Rosenblum
Robert McKee
Richard Rubin
AT&T
Room 3254A2
295 N. Maple Avenue
Basking Ridge, NJ 07920

John Goodman
Stephen Bozzo
Bell Atlantic
1710 H Street, N.W.
Washington, D.C. 20006

Robert Sutherland
Richard Sbaratta
Helen Schockey
Bell South
675 Peachtree Street, N.E.
Atlanta, GA 30375

Michael Altschul
CTIA
1133 21st Street, N.W.
Third Floor
Washington, D.C. 20036

Kenneth Hoffman
Floyd Self
P. O. Box 1876
Tallahassee, FL 32302
Counselor for Florida Pay
Telephone Assn.

David Gudino
GTE
1850 M Street, N.W.
Suite 1200
Washington, D.C. 20036

Douglas Brent
IXC Toll Fraud Subcommittee
9300 Shelbyville Road
Suite 700
Louisville, KY 40222

Brian Moir
1255 23rd Street, N.W.
Suite 800
Washington, D.C. 20037
Counsel fo ICA

Steven Hogan
Link USA Corp.
230 Second Street, S.E.
Suite 400
Cedar Rapids, IA 52401

Mary Sisak
Donald Elardo
MCI
1800 Pennsylvania Ave., N.W.
Washington, D.C. 20006

Anne MacClintock
SNET
227 Church Street
New Haven, CT 06510

David Cosson
Steven Watkins
NTCA
2626 Pennsylvania Ave., N.W.
Washington, D.C. 20037

James Ellis
William Free
Paula Falks
Southwestern Bell
175 East Houston
Room 1218
San Antonio, TX 78205

Albert Kramer
Robert Aldrich
Keck, Mahin & Cate
1201 New York Avenue, N.W.
Penthouse Suite
Washington, D.C. 20005
Counsel for NATA

Charles Hunter
Kelly, Hunter, Mow & Povich
1133 Connecticut Avenue, N.W.
Seventh Floor
Washington, D.C. 20036
Counsel for TRAA

Edward Wholl
William Balcerski
NYNEX
120 Bloomington Road
White Plains, NY 10605

Kathryn Marie Krause
US West
Suite 700
1020 19th Street, N.W.
Washington, D.C. 20036

James Tuthill
Nancy Woolf
Pacific Bell/Nevada Bell
140 New Montgomery Street
Room 1523
San Francisco, CA 94105

Bob McCoy
Shawna Barnard
Wiltel
Suite 3600
One Williams Center
Tulsa, OK 74172

Michael O'Connell
XIOX Corporation
577 Airport Boulevard
Suite 700
Burlingame, CA 94010

Jeffrey Lord
Flex Communications
4 Wells Street
P.O. Box 267
Johnstown, NY 12095

Gary Jensen
ISLUA-UAC
468 Shannon Square #9
Sulphur Springs, TX 75482

John Lyluk
Masco Corporation
21001 Van Born Road
Taylor, MI 48180

Paul Markes
Stormont-Vail Regional
Medical Center
1500 SW 10th Avenue
Topeka, KS 66604
Tina Rothrault
St. Margaret Memorial Hosp.
815 Freeport Road
Pittsburgh, PA 15215

Wendy Lucas
Pottstown Memorial Medical
Center
1600 E. High Street
Pottstown, PA 19464
Vicki Alexander
Primus
P.O. Box 111897
Nashville, TN 37222

Peter Jela
513 Bancorp
Cincinnati, OH

C. Bryan Tonet
Blue Cross/Blue Shield
444 Westminster St.
Providence, RI 02903

Jean Conley
Cooper Industries
P. O. Box 4999
Syracuse, NY 13221

Judith Johnson
McKenna & Cuneo
1575 Eye Street, N.W.
Washington, D.C. 20005

William Hughes
Union Central Life Ins. Co.
P. O. Box 179
Cincinnati, OH 45201

Martin Trauke
Raleigh Technology Group
Suite 907, The Forum
8601 Six Forks Road
Raleigh, NC 27615

Frank Guagenti
Matsushita Electric Corp.
9401 W. Grand Avenue
Franklin Park, IL 60131

Rosalyn Harris
Preformed Line Products
P. O. Box 91129
Cleveland, OH 44101

Alisa Evans
Caterpillar
2500 NC 42 East
P.O. Box 999
Clayton, NC 27520

Margaret Weitzel
Wyse Advertising
24 Public Square
Cleveland, OH 44113

Patti Evans
Chicago Convention and
and Tourism Bureau
McCormick Place-On-the-Lake
2301 S. Lake Shore Drive
Chicago, IL 60616

Mary Ellen Myers
JR Simplot Co.
5383 Irving Street
Boise, ID 83706

Mary Ann Postel
ILC Data Device Corp.
105 Wilbur Place
Bohemia, NY 11716

Betty Huntsman
KUTV Inc.
P.O. Box 30901
Salt Lake City, UT 84130

Joyce Amburgey
CSE Insurance Group
989 Market Street
San Francisco, CA 94103

James Blaszk
Patrick Whittle
Susan Jones
Gardner, Carton & Douglas
1301 K Street, N.W.
Suite 900 East
Washington, D.C. 20005
Counsel for Ad Hoc

John Bartlett
Robert Butler
Aliza Katz
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006
Counsel for Arinc

Genevieve Morelli
Comptel
1140 Connecticut Ave., N.W.
Suite 220
Washington, D.C. 20036

Wayne Black
C.Douglas Jarrett
Michael Bennett
Keller & Heckman
1001 G Street, N.W.
Suite 500 West
Washington, D.C. 20001
Counsel for API

David Jatlow
Young & Jatlow
2300 N Street, N.W.
Suite 600
Washington, D.C. 20037
Counsel for Ericsson Corp.

Debra Lagapa
Levine, Lagapa & Block
1200 19th Street, N.W.
1200 19th Street, N.W.

William Wyrrough
Florida PSC
101 E. Gaines Street
Tallahassee, FL 32399

Alfred Whittaker
Kirkland and Ellis
655 15th Street, N.W.
Suite 1200
Washington, D.C. 20005
Counsel for FMC Corp.

Keith Roland
Roland, Fogel, Koplentz & Carr
One Columbia Place
Albany, NY 12207
Counsel for IPANY